House Panel Passes Computer Security Training Bill

By Eric Fredell
GCN Staff

A bill to establish a computer-security training program at the National Bureau of Standards, opposed by the Reagan administration, was recently amended and approved by a House panel.

The amended bill is the latest effort by the subcommittee's chairman, Rep. Jack Brooks (D-Texas), to clarify the government's computer security guideiines. Brooks and other members of Congress have expressed concern about a presidential directive that places the lead computer-security role in the hands of the Defense Department.

The bill, HR 2889, was opposed by administration officials at a September hearing [*GCN*, Oct. 11] held by the Government Operations Subcommittee on Legislation and National Security because it would duplicate portions of National Security Decision Directive 145, signed by President Reagan last year.

That directive gives DOD undue control of unclassified information stored in civilian agency computers, Brooks has argued. He also has argued the directive conflicts with existing statutes, including the Brooks Act, that put the Office of Management and Budget, the General Services Administration and NBS in control of civilian-agency computer security.

The amended bill would divide the security roles of NBS and DOD more clearly, giving NBS authority over unclassified information and putting classified information under DOD's purview. The bill would also establish a Computer and Telecommunications and Security Advisory Board, appointed by the secretary of Commerce, to represent industry, government technical experts and federal managers.

The Reagan administration opposed the amended bill at a hearing held jointly by the House Science and Technology Subcommittee on Transportation, Aviation and Materials and the Subcommittee on Science, Research and Technology. Although intended to discuss the original version of HR 2889, the hearing focused considerable attention on the amended version, which the Government Operations Committee approved the day before.

Robert Brotzman, who heads the National Security Agency's National Computer Security Center, told the subcommittee that the amended bill "would upset the apple cart." He said the security center has "a number of activities under way that we believe, along with activities in other agencies, are addressing the concern that prompted HR 2889."

He said the amended version looked like "a rewrite of [NSDD] 145 into law, only under Commerce" instead of DOD. Such a change, if approved, "would cause a delay while we figured out exactly what the roles would shake out to be," Brotzman warned.

No matter who takes charge of federal computer security, the General Accounting Office's William Franklin said training is badly needed in the government. He said that a review of 25 mission-critical systems operated in 17 federal agencies revealed that only two have a formal security training program.

Franklin reiterated testimony presented by GAO at an earlier hearing on the bill held by Brooks' subcommittee. He said the bill overlaps with provisions contained in National Security Decision Directive 145, which places computer security authority in the hands of several committees.

While supporting the "intent of HR 2889," Franklin recommended "that a clear understanding of DOD's role vs. the roles of OMB, GSA and NBS be established in conjunction with consideration of HR 2889."

Brotzman downplayed the significance of DOD taking a lead role in government computer security. He said NSDD 145 does not give DOD "control" of civilian-agency or private-sector data but puts the department "in a leadership role to help develop and make available to all of us better [security] techniques."

Brotzman described a number of computer security efforts under way at the national center, including agency-specific training sessions.

James Burrows, director of NBS' Institute for Computer Sciences and Technology, said there is some confusion about who has control in the computer security area with the addition of NSDD 145 to other existing statutes. He said agencies have had a mixed response to the directive; they are pleased something is being done and are asking why DOD had to be put in charge.

He said NBS and DOD, including the security center, work closely in the computer security area and argued that NSDD 145 has had "no adverse affect" on NBS. He said the bill would probably push his department to spend a larger percentage of its budget — currently 10 percent or $1 million — on computer security.

Dial-Up Security Is Available, but Costly

By Arnold S. Levine
GCN Staff

GAITHERSBURG, Md. — One of the most common ways of getting into someone else's computer system is [illegible] ordinary dial-up telephone.

Hardware is available that can prevent dial-up access, and systems managers now face some difficult choices: They must decide whether a computer system needs better dial-up [illegible] such security should be one- or two-ended and how far such devices are valid security devices in

available. They refuse to operate as normal modems for dial-up purposes until the user enters a specified password. Users have no control over the connection information stored in the modems, and security manag- [illegible] they wish.

STAT